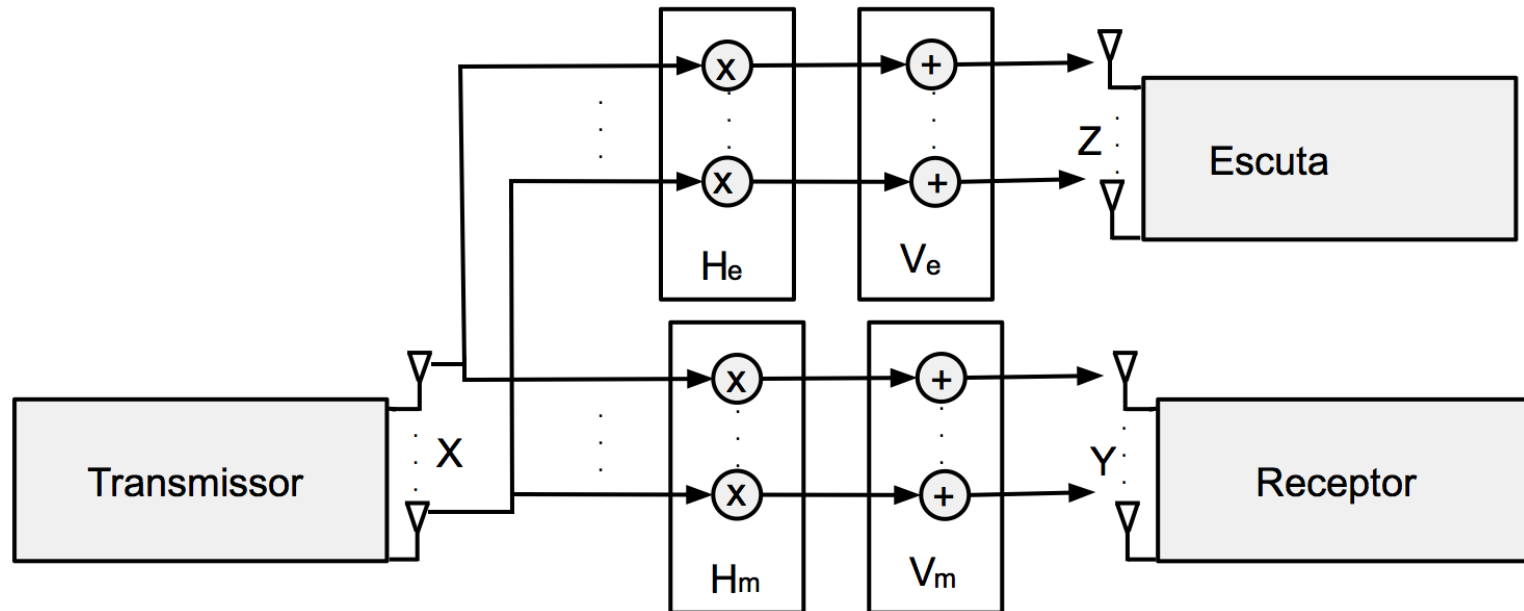


# Ergodic Secrecy Capacity in the MIMOME channel

André Saito Guerreiro – Unicamp  
Orientador: Gustavo Fraidenraich – Unicamp



- Channel Equations

$$Y = H_m X + V_m \quad H_m, H_e - \textit{Rayleigh}$$

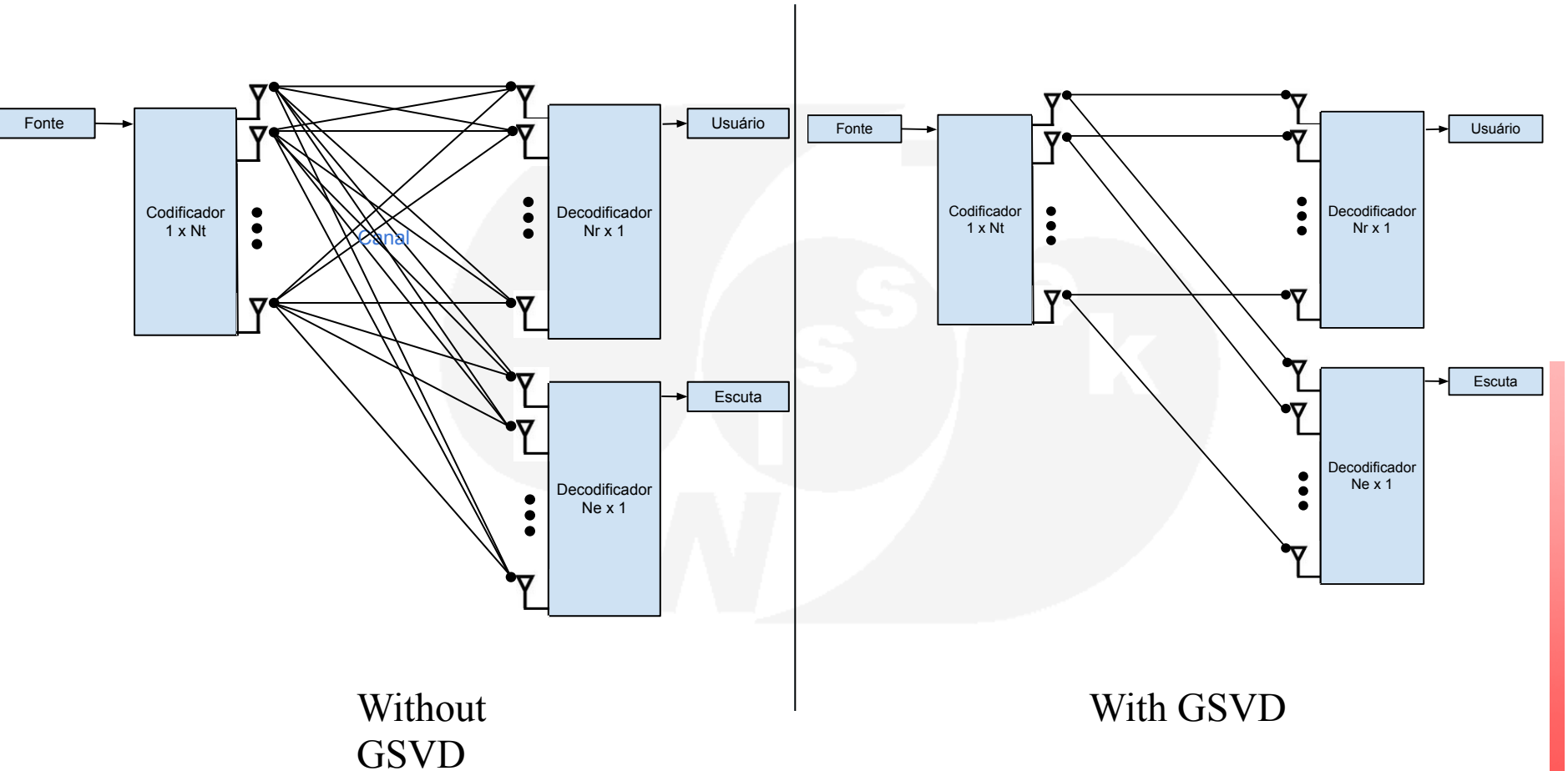
$$Z = H_e X + V_e \quad V_m, V_e - \textit{Gaussian}$$

- Secrecy Capacity Upper Bound

$$C_s \leq \sum_{j: \sigma_j^2 \geq 1}^q \log \sigma_j^2$$

- Equality at the High-SNR regime
- Is achievable through the use of a GSVD (Generalized singular value decomposition)- Requires CSITR of main and eavesdropper channel

# GSVD Based transmission



- Ergodic Secrecy capacity

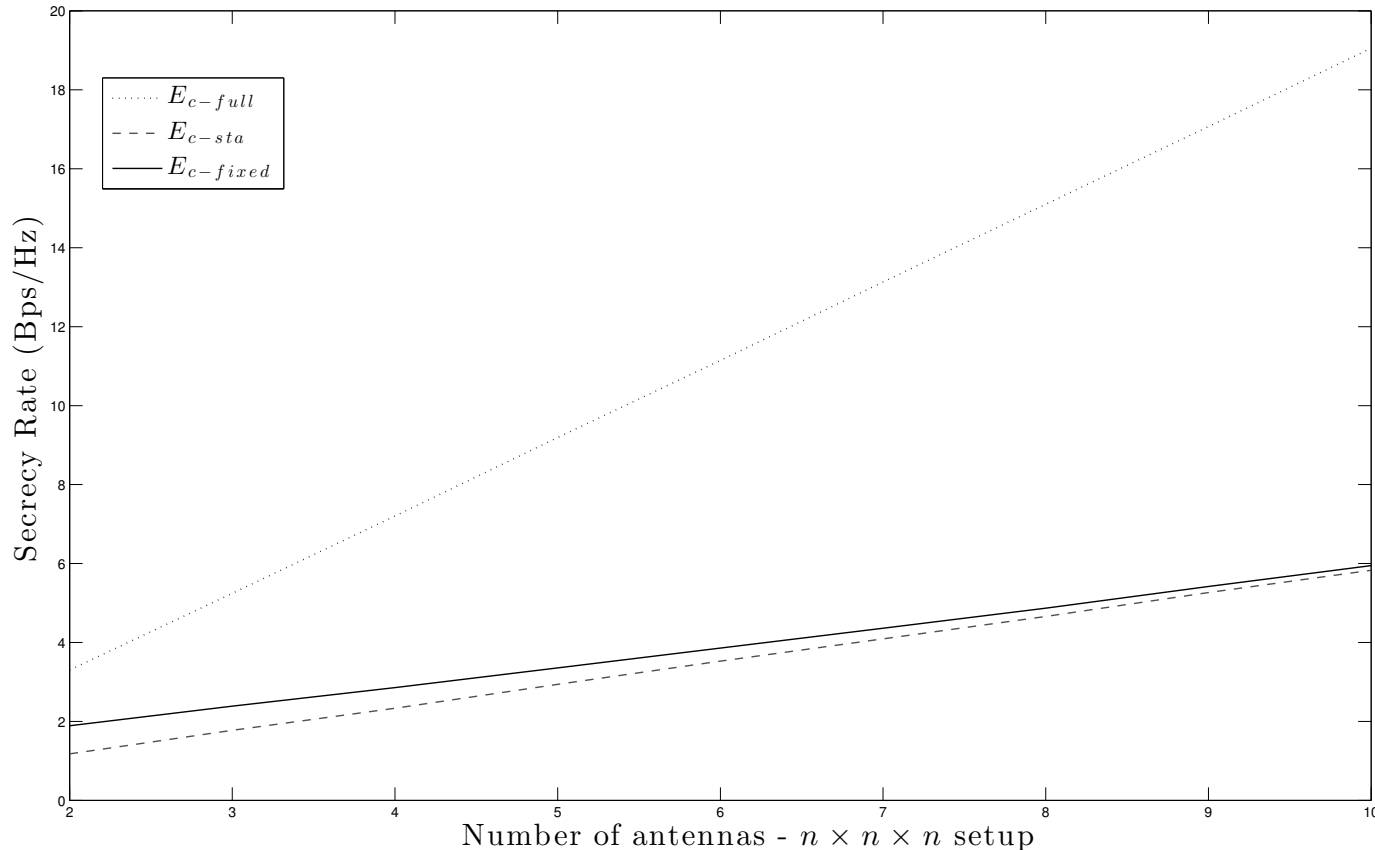
$$C_s = \mathbb{E}_{\sigma_j^2} \left[ \sum_{j: \sigma_j^2 > 1}^{n_t} \log \sigma_j^2 \right]$$

$$E_{C_{-full}} = \sum_{k=0}^{n_t-1} \sum_{l=0}^k \sum_{u=0}^k \left[ h_{k,u,l,n_r,n_t} \left( \left( \frac{\rho_m}{\rho_e} \right)^4 (l + n_r - n_t + u + 1) \left( \left( \frac{\rho_m}{\rho_e} \right)^4 + 1 \right)^{l+n_r+u+1} \right. \right. \\ \times {}_3F_2 \left( 1, 1, l + n_r - n_t + u + 2; 2, 2; - \left( \left( \frac{\rho_m}{\rho_e} \right)^4 \right) \right) \\ \left. \left. + 2 \ln \left( \frac{\rho_m}{\rho_e} \right) \left( -\frac{\rho_m}{\rho_e} \right)^4 \left( \left( \frac{\rho_m}{\rho_e} \right)^4 + 1 \right)^{l+n_r+u} \right. \right. \\ \left. \left. - \left( \left( \frac{\rho_m}{\rho_e} \right)^4 + 1 \right)^{l+n_r+u} + \left( \left( \frac{\rho_m}{\rho_e} \right)^4 + 1 \right)^{n_t} \right) \left( \left( \frac{\rho_m}{\rho_e} \right)^4 + 1 \right)^{-l-n_r-u-1} \right],$$

and

$$h_{k,u,l,n_r,n_t} = (-k)_l (k + n_r - n_t + 1)_l (l + n_r - n_t + 1)_{k-l} (-k)_u (k + n_r - n_t + 1)_u \\ b_{k,n_r,n_t}^{-1} (n_r - n_t + u + 1)_{k-u} (\ln(2)(k!)^2 l! u! (l + n_r - n_t + u + 1)^{-1},$$

# Comparing full CSITR with statistical CSI



- Conclusion- CSITR is a key factor in increasing ergodic secrecy capacity at High-SNR